Claims

1. In a data processing operation having stored data in a plurality of data files, a system for protecting said data files from unauthorized users comprising:

means for receiving user requests for access to data files;

means for determining whether said requests are unauthorized intrusions into said requested data files; and

means responsive to a determination that a request is unauthorized for destroying the requested data files.

2. The data processing operation system of claim 1 further including means for storing for each of said plurality of data files, a backup file inaccessible to user requests.

3. The data processing operation system of claim 2 further including means for reloading a backup file for each destroyed file.

4. The data processing operation system of claim 1 wherein said means for determining whether said user requests are unauthorized intrusions include:

means for determining whether a user access identification code has been denied; and

means for determining whether the user has copied the requested files.

5. In a communication network with access to a plurality of network sites each having stored data in a plurality of data files accessible in response to requests from users at other sites in the network, a system for protecting said network site data files from unauthorized users comprising:

means associated with a network site for receiving user requests for access to data files;

means at said network site for determining whether said user requests are unauthorized intrusions into said requested data files; and

means at said network site responsive to a determination that a request is unauthorized for destroying the requested data files.

6. The communication network system of claim 5 further including means for storing for each of said plurality of data files at said network site, a backup file inaccessible to user requests.

7. In a World Wide Web communication network with access to a plurality of open Web sites each having stored data in a plurality of data files accessible in response to requests from users at stations throughout the Web, a system for protecting said open Web site data files from unauthorized users comprising:

means associated with an open Web site for receiving user requests for access to data files;

means at said open Web site for determining whether said user requests are unauthorized intrusions into said requested data files; and

means at said open Web site responsive to a determination that a request is unauthorized for destroying the requested data files.

8. The World Wide Web communication network system of claim 7 further including means for storing for each of said plurality of data files at said open Web site, a backup file inaccessible to user requests.

9. The World Wide Web communication network system of claim 8 further including means for reloading a backup file for each destroyed file.

10. In a data processing operation having stored data in a plurality of data files, a method for protecting said data files from unauthorized users comprising:

receiving user requests for access to data files;

determining whether said requests are unauthorized intrusions into said requested data files; and

destroying the requested data files responsive to a determination that a request is unauthorized.

11. The data processing method of claim 10 further including the step of storing for each of said plurality of data files, a backup file inaccessible to user requests.

12. The data processing method of claim 11 further including the step of reloading a backup file for each destroyed file.

13. The data processing method of claim 10 wherein said step of determining whether said user requests are unauthorized intrusions includes:

determining whether a user access identification code has been denied; and

determining whether the user has copied the requested files.

14. In a communication network with access to a plurality of network sites each having stored data in a plurality of data files accessible in response to requests from users at other sites in the network, a method for protecting said network site data files from unauthorized users comprising:

receiving user requests for access to data files at a network site;

determining at said network site whether said user requests are unauthorized intrusions into said requested data files; and

destroying the requested data files responsive to a determination that a request is unauthorized.

15. The communication network method of claim 14 further including the step of storing for each of said plurality of data files at said network site, a backup file inaccessible to user requests.

16. The communication network method of claim 15 further including the step of reloading a backup file for each destroyed file.

17. In a World Wide Web communication network with access to a plurality of open Web sites each having stored data in a plurality of data files accessible in response to requests from users at stations throughout the Web, a method for protecting said open Web site data files from unauthorized users comprising:

receiving user requests for access to data files at said open Web site;

determining whether said user requests are unauthorized intrusions into said requested data files at said open Web site; and

destroying the requested data files at said open Web site responsive to a determination that a request is unauthorized.

18. The World Wide Web communication network method of claim 17 further including the step of storing for each of said plurality of data files at said open Web site, a backup file inaccessible to user requests.

19. The World Wide Web communication network method of claim 18 further including the step of reloading a backup file for each destroyed file.

20. The World Wide Web communication network method of claim 17 wherein said step of determining whether said user requests are unauthorized intrusions includes:

determining whether a user access identification code has been denied; and

determining whether the user has copied the requested files.

21. A computer program having code recorded on a computer readable medium for protecting data files from unauthorized users in a data processing operation having stored data in a plurality of data files, said program comprising:

means for receiving user requests for access to data files;

means for determining whether said requests are unauthorized intrusions into said requested data files; and

means responsive to a determination that a request is unauthorized for destroying the requested data files.

22. The computer program of claim 21 further including means for storing for each of said plurality of data files, a backup file inaccessible to user requests.

23. The computer program of claim 22 further including means for reloading a backup file for each destroyed file.

24. The computer program of claim 21 wherein said means for determining whether said user requests are unauthorized intrusions include:

means for determining whether a user access identification code has been denied; and

means for determining whether the user has copied the requested files.

25. A computer program having code recorded on a computer readable medium for protecting data files from unauthorized users in a communication network with access to a plurality of network sites each having stored data in a plurality of data files accessible in response to requests from users at other sites in the network, said program comprising:

means associated with a network site for receiving user requests for access to data files;

means at said network site for determining whether said user requests are unauthorized intrusions into said requested data files; and

means at said network site responsive to a determination that a request is unauthorized for destroying the requested data files.

26. The computer program of claim 25 further including means for storing for each of said plurality of data files at said network site, a backup file inaccessible to user requests.

27. A computer program having code recorded on a computer readable medium for protecting open Web sites in a World Wide Web communication network with access to a plurality of open Web sites each having stored data in a plurality of data files accessible in response to requests from users at stations throughout the Web, said program comprising:

means associated with an open Web site for receiving user requests for access to data files;

means at said open Web site for determining whether said user requests are unauthorized intrusions into said requested data files; and

means at said open Web site responsive to a determination that a request is unauthorized for destroying the requested data files.

28. The computer program of claim 27 further including means for storing for each of said plurality of data files at said open Web site, a backup file inaccessible to user requests.

29. The computer program of claim 28 further including means for reloading a backup file for each destroyed file.

30. The computer program of claim 27 wherein said means for determining whether said user requests are unauthorized include:

means for determining whether a user access identification code has been denied; and

means for determining whether the user has copied the requested files.